AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A cryptographic method, ~~during which an integer division of a type q = a div b and/or a modular reduction of a type r = a mod b is performed, where q is a quotient, a is a number containing m bits, b is a number containing n bits, with n less than or equal to m and b_{n-1} is non-zero, b_{n-1} being the most significant bit of the number b,~~ comprising the steps of:

performing an integer division of a type q = a div b and/or a modular reduction of a type r = a mod b by a processor, where q is a quotient, a is a number containing m bits, b is a number containing n bits, with n less than or equal to m and b_{n-1} is non-zero, b_{n-1} being the most significant bit of the number b;

masking the number a by a random number ρ by the processor before performing the integer division and/or the modular reduction[[,]] ;

taking away the contribution made by the random number ρ from the result of the integer division after having performed the integer division; and

generating encrypted or decrypted data by the processor in accordance with a result of the division and/or modular reduction.

2. (Previously Presented) A method according to claim 1, wherein, in order to mask the number a, b times the random number ρ (a <- a + b*ρ) is added to the number a.

3. (Canceled)

4. (Currently Amended) A method according to claim [[3]] 1, wherein, in order to take away the contribution made by the random number ρ, said random number ρ is subtracted from the result of the integer division.

5. (Previously Presented) A method according to claim 1, wherein the random number ρ is modified at each implementation of the method.

6. (Previously Presented) A method according to claim 1, wherein the random number ρ is modified after a predetermined number of implementations of the method.

7. (Previously Presented) An electronic component comprising means for implementing a method according to claim 1, said means comprising a plurality of registers for storing the numbers a and b.

8. (Previously Presented) A chip card comprising a component according to claim 7.